CLAIMS:

1. In a digital rights managment system in which a digital license confers predetermined usage rights in relation to a digital content, a method of transferring the usage rights from a first content player application to a second content player application, including the steps of:

a) associating with the first content player application a first status indication with respect to the digital license for indicating whether the first player application is entitled to exercise the usage rights conferred by the license;

b) associating with the second content player application a second status indication with respect to the digital license for indicating whether the second player application is entitled to exercise the usage rights conferred by the license;

c) transmitting a request for transfer of the usage rights from the second player application to the first player application;

d) setting the first status indication to indicate that the first player application is no longer entitled to exercise the usage rights;

e) transmitting a response transferring the usage rights from the first player application to the second player application; and

f) setting the second status indication to indicate that the second application is henceforth entitled to exercise the usage rights,

wherein the steps (c) to (f) are carried out in the stated order.

2. The method of claim 1 wherein the first content player application executes on a first player device and the second content player application executes on a second player device.

3. The method of either one of the preceding claims wherein prior to the step of transmitting a request the first status indication indicates that the first content player application is entitled to exercise the usage rights.

4. The method of any one of the preceding claims wherein if the step (e) of transmitting a response is not successfully completed within a predetermined time

following the completion of the step of transmitting a request, the transfer of usage rights is aborted.

5. The method of any one of the preceding claims wherein step (c) includes, after transmitting the request, setting the second status indication to indicate that the transfer of the usage rights has been requested.

6. The method of claim 5 wherein the step of transmitting the request includes transmitting a request message from the second content player application to the first content player application, the message including the value of the second status indication.

7. The method of either one of claims 5 or 6 further including the step of determining if the transfer of rights was aborted by checking the values of the first and second status indications to establish if the second content player application has requested the usage rights and the first content player application is no longer entitled to exercise the usage rights.

8. The method of any one of claims 1 to 7 wherein a plurality of status indications are associated with each of said first and second content player applications, corresponding with a plurality of digital licenses.

9. The method of claim 8 further including the step of computing an authentication code that is a function of the values of the respective status indicators associated with each of the first and second content player applications each time a status indication associated with the corresponding content player applications is altered.

10. The method of claim 9 wherein the authentication code is computed as a one-way hash function of all of the respective status indication values.

11. The method of claim 10 further including the step of associating a secret key with each one of said first and second content player applications, wherein

the authentication code is computed as a function of the corresponding status indication values and said secret key.

12. The method of claim 11 wherein the authentication code is computed as a function of the corresponding status indication values and the current value of a secure monotonic counter associated with the respective content player application, said counter being incremented each time any status indication is altered.

13. The method of any one of the preceding claims wherein the step of transmitting a response includes transmitting the digital license from the first player application to the second player application.

14. The method of claim 13 wherein the digital license includes a validated portion including characteristic information of a digital content decryption key that is required for decrypting the digital content, and an unvalidated portion including the digital content decryption key encrypted using an encryption key associated with the first digital content player application, and wherein transmitting the digital license from the first player application to the second player application includes the steps of:

decrypting the digital content decryption key using a decryption key associated with the first digital content player application;

using the decrypted digital content decryption key to generate the characteristic information of the digital content decryption key;

verifying that the generated characteristic information matches the characteristic information included in the validated portion of the first digital license; and

if the verification is successful, encrypting the digital content decryption key using an encryption key associated with said second digital content player application and including said encrypted key in the unvalidated portion of the digital license to be transmitted to the second player application.

15. In a digital rights management system in which a digital license confers predetermined usage rights in relation to a digital content, a system for transferring the usage rights from a first content player application to a second content player application, including:

request transmitting means adapted to transmit a request for transfer of the usage rights from the second player application to the first player application;

first indication setting means adapted to set a first status indication associated with said first content player application to indicate that the first player application is no longer entitled to exercise the usage rights;

response transmitting means adapted to transmit a response transferring the usage rights from the first player application to the second player application; and

second indication setting means adapted to set a second status indication associated with said second content player application to indicate that the second application is henceforth entitled to exercise the usage rights.

16. The system of claim 15 including first and second content player devices, wherein the first device includes said first indication setting means and said response transmitting means, and the second device includes said request transmitting means and said second indication setting means.

17. The system of either one of claims 15 or 16 further including:

request receiving means adapted to receive a request for transfer of the usage rights transmitted from the second player application at the first player application; and

response receiving means adapted to receive a response transferring the usage rights transmitted from the first player application at the second player application.

18. The system of any one of claims 15 to 17 further including a timer arranged to measure a predetermined time-out period following the transmission of a request for transfer of the usage rights from the second player application, and whereby the system is adapted to abort the transfer of usage rights if a

corresponding response is not received by the response receiving means prior to the expiry of said predetermined time-out period.

19. The system of any one of claims 15 to 18 wherein the request transmitting means is adapted to transmit a request message that includes the value of the second status indicator.

20. The system of any one of claims 15 to 19 further including authentication code computing means adapted to compute an authentication code that is a function of the value of at least one of the first and second status indications, each time the value of the corresponding status indication is altered.

21. The system of claim 20 wherein the authentication code computing means computes the authentication code as a one-way hash function including the value of the corresponding status indication.

22. The system of claim 21 wherein the authentication code computing means computes the authentication code as a function of the value of the corresponding status indication and a secret key.

23. The system of claim 22 including secure storage for storing the value of the secret key.

24. The system of either one of claims 22 or 23 further including a secure monotonic counter associated with each of said first and second content player applications, each secure monotonic counter being incremented each time a status indication associated with the corresponding application is altered, wherein the authentication code computing means computes the authentication code as a function of the value of the corresponding status indication and the current value of the corresponding secure monotonic counter.

25. The system of any one of claims 15 to 24 further including first and second tracking files associated respectively with said first and second content player

applications, wherein the first and second status indications are implemented as transaction flags stored in said tracking files.

26. The system of claim 25 including a plurality of tracking flags corresponding with a plurality of digital licenses, wherein the transaction flags are associated with the corresponding digital licenses by using a unique license identifier stored within the license as an index in said tracking files.

27. The system of any one of claims 15 to 26 which is implemented, at least in part, using one or more tamper resistant secure computing devices.

28. The system of any one of claims 15 to 27 including license transmitting means adapted to transmit the digital license from the first player application to the second player application.

29. The system of claim 28 wherein the digital license includes a validated portion and an unvalidated portion, the validated portion including characteristic information of a digital content decryption key that is required to decrypt the digital content, and the unvalidated portion including the digital content decryption key encrypted using an encryption key associated with the first digital content player application, and the system further including:

digital content decrypting means adapted to decrypt the digital content decryption key using a decryption key associated with the first digital content player application;

generating means adapted to generate the characteristic information of the digital content decryption key using the decrypted digital content decryption key;

verification means adapted to verify that the generated characteristic information matches the characteristic information included in the validated portion of the first digital license; and

encryption means adapted to, if the verification is successful, encrypt the digital content decryption key using an encryption key associated with said second digital content player application and to include said encrypted key in the

unvalidated portion of the digital license to be transmitted to the second digital content player application.

30. In a digital rights management system in which a digital license confers predetermined usage rights in relation to a digital content, a method of a first digital content player device transferring the usage rights to a second digital content player device, including the steps of:

a) receiving a request from the second player application to transfer the usage rights from the first player application to the second player application;

b) setting a first status indication to indicate that the first player application is no longer entitled to exercise the usage rights conferred by the license; and

c) transmitting a response transferring the usage rights from the first player application to the second player application, whereby upon receipt of said response the second player application sets a second status indication to indicate that the second player application is henceforth entitled to exercise the usage rights,

wherein the steps (a) to (c) are carried out in the stated order.

31. The method of claim 30 wherein prior to step (a) the first status indication indicates that the first content player application is entitled to exercise the usage rights.

32. The method of either one of claims 30 or 31 wherein the step (c) must be successfully completed within a predetermined time following the completion of step (a), otherwise the transfer of usage rights is aborted.

33. The method of any one of claims 30 to 32 further including the step of computing an authentication code that is a function of the value of the first status indication each time the value of the first status indication is altered.

34. The method of claim 33 wherein the authentication code is computed as a one-way hash function of the value of the first status indication.

35. The method of either one of claims 33 or 34 wherein the authentication code is computed as a function of the value of the first status indication and a secret key.

36. The method of any one of claims 33 to 35 wherein the authentication code is computed as a function of the value of the first status indication, and the current value of a secure monotonic counter that is incremented each time the value of the first status indication is altered.

37. In a digital rights management system in which a digital license confers predetermined usage rights in relation to a digital content, a method of a second digital content player device transferring the usage rights from a first digital content player device, including the steps of:

a) transmitting a request to the first content player device to transfer the usage rights to the second content player device, whereby the first device sets a first status indication to indicate that the first device is no longer entitled to exercise the usage rights conferred by the license;

b) receiving a response transferring the usage rights from the first content player device to the second content player device; and

c) setting a second status indication to indicate that the second content player device is henceforth entitled to exercise the usage rights;

wherein the steps (a) to (c) are carried out in the stated order.

38. The method of claim 37 wherein prior to step (a) the second status indication indicates that the second content player device is not entitled to exercise the usage rights.

39. The method of either one of claims 37 or 38 wherein the step (c) must be successfully completed within a predetermined time following the completion of step (a), otherwise the transfer of usage rights is aborted.

40. The method of any one of claims 37 to 39 further including the step of computing an authentication code that is a function of the value of the second status indication each time the value of the second status indication is altered.

41. The method of claim 40 wherein the authentication code is computed as a one-way hash function of the value of the second status indication.

42. The method of either one of claims 40 or 41 wherein the authentication code is computed as a function of the value of the second status indication and a secret key.

43. The method of any one of claims 40 to 42 wherein the authentication code is computed as a function of the value of the second status indication and the current value of a secure monotonic counter that is incremented each time the value of the second status indication is altered.

44. A digital content player device for use in a digital rights management system in which a digital license confers predetermined usage rights in relation to a digital content, the device including:

request transmitting means adapted to transmit a request for transfer of the usage rights from another device to said digital content player device;

response transmitting means adapted to transmit a response to a request for transfer of the usage rights received by said digital content player device from another device;

request receiving means for receiving a request for transfer of the usage rights by said digital content player device from another device;

response receiving means for receiving a response by said digital content player device from another device to a transmitted request for transfer of the usage rights; and

indication setting means adapted to set a status indication to indicate that said digital content player device is entitled to exercise the usage rights when the rights are transferred to the digital content player device, and to indicate that the

digital content player device is not entitled to execute the usage rights when the rights have not been transferred to the digital content player device.

45. The digital content player device of claim 44 further including a timer configured to measure a predetermined time-out period following the transmission of a request for transfer of the usage rights by the request transmitting means, and wherein the digital content player device is adapted to abort the transfer of usage rights if a corresponding response is not received by the response receiving means prior to the expiry of said time-out period.

46. The digital content player device of either one of claims 44 or 45 including authentication code computing means adapted to compute an authentication code that is a function of the value of said status indication each time the value of the status indication is altered.

47. The digital content player device of claim 46 wherein the authentication code is computed as a one-way hash function of the value of the status indication.

48. The digital content player device of either one of claims 46 or 47 wherein the authentication code is computed as a function of the value of the status indication and a secret key.

49. The digital content player device of claim 48 further including secure storage for storing the secret key.

50. The digital content player device of any one of claims 46 to 49 further including a secure monotonic counter that is incremented each time the status indication is altered, and wherein the authentication code is computed as a function of the value of the status indication and the current value of the secure monotonic counter.

51. The digital content player device of any one of claims 44 to 50 further including a tracking file, wherein the status indication is implemented as a transaction flag stored in said tracking file.

52. The digital content player device of claim 51 wherein the tracking file includes a plurality of transaction flags corresponding with a plurality of digital licenses, wherein each said transaction flag is associated with the corresponding digital license by using a unique license identifier stored within the license as an index in the tracking file.

53. In a digital rights management system, a method for generating a second digital license from a first digital license, wherein said first digital license confers predetermined usage rights in relation to a digital content upon a first digital content player application and said second digital license confers the usage rights upon a second digital content player application, said digital content being normally encrypted and only able to be decrypted using a digital content decryption key, the first and second digital licenses each including a validated portion and an unvalidated portion, wherein

the validated portion of the first digital license includes characteristic information of the digital content decryption key, and

the unvalidated portion of the first digital license includes the digital content decryption key encrypted using an encryption key associated with said first digital content player application,

the method including the steps of:

decrypting the digital content decryption key using a decryption key associated with the first digital content player application;

using the decrypted digital content decryption key to generate the characteristic information of the digital content decryption key;

verifying that the generated characteristic information matches the characteristic information included in the validated portion of the first digital license; and

if the verification is successful, encrypting the digital content decryption key using an encryption key associated with said second digital content player

application and including said encrypted key in the unvalidated portion of the second digital license.

54. The method of claim 53 further including the step of verifying that the validated portion of the first digital license has not been altered or falsified.

55. The method of claim 54 wherein the validated portion of the first digital license is validated with a digital signature of a trusted authority, and the step of verifying that the validated portion of the first digital license has not been altered or falsified includes verifying that the digital signature is correct with respect to the trusted authority and the contents of the validated portion of the license.

56. The method of either claim 54 or claim 55 further including the step of rejecting the digital license if the license has been altered or falsified.

57. The method of any one of claims 53 to 56 wherein the validated portion of the first digital license includes characteristic information of the encrypted digital content, and the method includes the further steps of:

generating the characteristic information of the encrypted digital content; and

verifying that the generated characteristic information matches the corresponding information included in the validated portion of the first digital license.

58. The method of any one of claims 53 to 57 wherein the encryption key associated with the first digital content player application is the public key of a first public/private key pair, and the step of decrypting includes using the corresponding private key to decrypt the encrypted digital content decryption key.

59. The method of claim 58 wherein the step of encrypting includes using a public key of a second public/private key pair that is associated with the second digital content player application to encrypt the digital content decryption key.

60. The method of any one of claims 53 to 59 wherein the characteristic information of the digital content decryption key is a hash of the digital content decryption key, and generating the characteristic information of the digital content decryption key includes computing the hash value of the digital content decryption key.

61. The method of claim 60 wherein the hash value is computed using a one-way, collision-free and pre-image resistant hash function.

62. In a digital rights management system, an apparatus for generating a second digital license from a first digital license, wherein said first digital license confers predetermined usage rights in relation to a digital content upon a first digital content player application and said second digital license confers the usage rights upon a second digital content player application, said digital content being normally encrypted and only able to be decrypted using a digital content decryption key, the first and second digital licenses each including a validated portion and an unvalidated portion wherein

the validated portion of the first digital license includes characteristic information of the digital content decryption key, and

the unvalidated portion of the first digital license includes the digital content decryption key encrypted using an encryption key associated with said first digital content player application,

the apparatus including:

decrypting means adapted to decrypt the digital content decryption key using a decryption key associated with the first digital content player application;

generating means adapted to use the decrypted digital content decryption key to generate the characteristic information of the digital content decryption key;

verifying means adapted to verify that the generated characteristic information matches the characteristic information included in the validated portion of the first digital license; and

encrypting means adapted to check if the verification is successful, and if so then to encrypt the digital content decryption key using an encryption key

associated with said second digital content player application and to include said encrypted key in the unvalidated portion of the second digital license.

63. The apparatus of claim 62 further including license verifying means adapted to verify that the validated portion of the digital license has not been altered or falsified.

64. The apparatus of claim 63 wherein the validated portion of the first digital license is validated with a digital signature of a trusted authority, and the license verifying means is adapted to verify that the digital signature is correct with respect to the trusted authority and the contents of the validated portion of the license.

65. The apparatus of any one of claims 62 to 64 wherein the validated portion of the digital license includes characteristic information of the encrypted digital content, and the content verifying means is adapted to generate the characteristic information of the encrypted digital content, and to verify that the generated characteristic information matches the corresponding information included in the validated portion of the digital license.

66. The apparatus of any one of claims 62 to 65 wherein the encryption key associated with the first digital content player application is the public key of a first public/private key pair, and the decrypting means is arranged to use the corresponding private key to decrypt the digital content decryption key.

67. The apparatus of claim 66 wherein the encrypting means is arranged to use the public key of a second public/private key pair that is associated with the second digital content player application to encrypt the digital content decryption key.

68. The apparatus of any one of claims 62 to 67 wherein the characteristic information of the digital content decryption key is a hash of the digital content decryption key, and the generating means is adapted to compute the hash value

of the digital content decryption key, and the verifying means is adapted to compare the computed hash value with the hash value included in the validated portion of the first digital license.

69. The apparatus of claim 68 wherein the generating means is adapted to compute a one-way, collision-free and pre-image resistant hash function of the digital content decryption key.